Network router data

Routers are the devices responsible for ensuring that traffic goes to the right network segment. Unlike switches that operate at Layer 2, routers work at Layer 3, directing traffic based on TCP/IP address and protocol (port number). Routers are responsible for particular Layer 3 address spaces and manage traffic using information in routing tables and configured policies. Routers exchange information and update their forwarding tables using dynamic routing protocols.

Network engineers use router logs and statistics to monitor traffic flow and ensure that traffic is being correctly forwarded between network segments. Data from routing protocol updates can show whether your routers are appropriately exchanging route tables with other locations, that external traffic can reach you, and that internal traffic is correctly forwarded to external routers. Router data can also be used to detect configuration changes and error or failure alerts correlating with security indicators.

Application

When your Splunk deployment is ingesting network router data, you can use it to accomplish security and compliance and IT Ops use cases.

- Managing Cisco IOS devices
- Finding large web uploads

Sources

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). In addition, these Splunk Add-Ons and Apps are helpful for working with network router data.

- Arista Networks Telemetry For Splunk
- Splunk Add-on for Forcepoint Web Security
- Splunk Add-on for McAfee Web Gateway
- Splunk Add-on for Cisco WSA
- Cisco Networks Add-on for Splunk Enterprise
- Splunk Add-on for Websense DLP


The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.